

Red Hat Security – Linux in Physical, Virtual, and Cloud

4 jours (28 heures)

Expertise

à partir de

3 740 € HT par personne (TVA en vigueur)

Contenu mis à jour le 25/09/2026. Document téléchargé le 02/10/2026.

Objectifs

À l'issue de cette formation, vous serez capable de :

- Analyser et corriger des problèmes de conformité du système à l'aide d'OpenSCAP et de SCAP Workbench
- Utiliser et adapter le contenu de politiques de référence fourni avec Red Hat Enterprise Linux
- Gérer les activités en lien avec la sécurité sur vos systèmes à l'aide de l'infrastructure d'audit du noyau
- Mettre en oeuvre des techniques SELinux avancées pour restreindre l'accès au niveau des utilisateurs, des processus et des machines virtuelles
- Déterminer l'intégrité des fichiers et leurs permissions avec l'utilitaire AIDE
- Bloquer l'utilisation de périphériques USB non autorisés à l'aide d'USBGuard
- Protéger des données au repos avec déchiffrement automatique sécurisé dès le démarrage avec NBDE
- Identifier des risques et des erreurs de configuration de façon proactive sur les systèmes et correction à l'aide de Red Hat Insights
- Analyser l'état de conformité et corriger à grande échelle à l'aide d'OpenSCAP, de Red Hat Insights, de Red Hat Satellite et de Red Hat Ansible Tower.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Administrateurs système, administrateurs de sécurité informatique, ingénieurs de sécurité informatique et autres professionnels chargés de la conception, de la mise en oeuvre, du maintien et de la gestion de la sécurité de systèmes Red Hat Enterprise Linux conformément aux politiques de sécurité en vigueur dans l'entreprise.

Prérequis

Etre titulaire de la certification RHCE (Ingénieur Certifié Red Hat), ou avoir des connaissances et/ou expérience(s) équivalentes de l'utilisation de Red Hat Enterprise Linux. Pour pouvoir suivre ce cours, il est impératif que chaque stagiaire se crée un identifiant (ID) sur le site de l'éditeur.

Afin de valider vos prérequis avant la formation, un QCM est disponible ; n'hésitez pas à nous contacter.

Programme

1 Pendant votre formation

Red Hat Security – Linux in Physical, Virtual, and Cloud

Gestion de la sécurité et des risques

- Définir des stratégies pour gérer la sécurité sur des serveurs Red Hat Enterprise Linux

Automatisation de la configuration et de la correction avec Ansible

- Corriger les problèmes de configuration et de sécurité à l'aide de playbooks Ansible

Protection des données avec LUKS et NBDE

- Chiffrer les données sur des périphériques de stockage avec LUKS
- Utiliser NBDE pour gérer le déchiffrement automatique lorsque les serveurs sont démarrés

Restriction de l'accès des périphériques USB

- Protéger le système contre l'accès des périphériques USB non autorisés grâce à USBGuard

Contrôle de l'authentification à l'aide de modules PAM (Pluggable Authentication Modules)

- Gérer les contrôles d'authentification, d'autorisation, de paramètres de session et de mots de passe en configurant des modules PAM

Enregistrement des événements système dans le système d'audit

- Enregistrer et analyser les événements système touchant à la sécurité à l'aide du sous-système d'audit du noyau Linux et d'outils complémentaires

Surveillance des changements au sein des systèmes de fichiers

- Détecter et analyser les modifications apportées aux systèmes de fichiers d'un serveur et à leur contenu avec l'utilitaire AIDE

Réduction des risques avec SELinux

- Renforcer la sécurité et le confinement des processus à l'aide de SELinux et de ses techniques et analyses avancées

Gestion de la conformité avec OpenSCAP

- Evaluer et corriger la conformité d'un serveur à l'aide de politiques de sécurité en utilisant OpenSCAP

Automatisation de la conformité avec Red Hat Satellite

- Automatiser et faire évoluer votre capacité d'effectuer des vérifications OpenSCAP
- Corriger les problèmes de conformité avec Red Hat Satellite

Analyse et correction des problèmes avec Red Hat Insights

- Détecter, identifier et corriger des problèmes et vulnérabilités courants sur des systèmes Red Hat Enterprise Linux avec Red Hat Insights

Révision approfondie

- Réviser le contenu de ce cours au travers d'exercices pratiques

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Accessibilité aux personnes en situation de handicap